

DETAILED ACTION

1. Claims 1-12 and 15 are allowed. Claims 1-12 and 15 are re-numbered as claims 1-13.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Steve Cha on 7/17/08.

The application has been amended as follows:

1. (Currently Amended) A Gigabit Ethernet-based passive optical network comprising:

an Optical Line Terminal (OLT) for receiving a public key through transmission medium, encrypting a secret key by means of the received public key, transmitting the encrypted secret key, encrypting data by means of the secret key, and transmitting the encrypted data, the OLT being located in a service provider-side; and

an Optical Network Terminal (ONT) for transmitting the public key to the OLT, receiving the encrypted secret key transmitted from the OLT, decrypting the encrypted secret key by means of a private key residing in an ONT key management unit of the ONT for managing a public key and at the private keys, receiving the encrypted data, and decrypting the received encrypted data by means of the decrypted ~~the~~ secret key,

wherein the public key is used for encrypting the secret key, the secret key is encrypted by means of the public key, and the data is encrypted by the OLT by means of the secret key.

10. (Currently Amended) An encryption method for transferring data between an Optical Line Terminal (OLT) and a plurality of Optical Network Terminals (ONTs) in a Gigabit Ethernet-based passive optical network ~~an E-PON structure~~, the encryption method comprising the steps of:

- a) transmitting, by the ONT, a public key to the OLT;
- b) encrypting, by the OLT, a secret key by means of the public key transmitted from the ONT and transmitting the encrypted secret key to the ONT;
- c) decrypting, by the ONT, the encrypted secret key transmitted from the OLT by means of a private key residing in the ONT in an ONT key management unit for managing a public key and the private key;
- d) encrypting, by the OLT, data by means of the secret key and transmitting the encrypted data to the ONT; and
- e) decrypting, by the ONT, the encrypted data transmitted from the OLT by means of the decrypted secret key.

12. (Currently Amended) An encryption method for transferring data between an Optical Line Terminal (OLT) and a plurality of Optical Network Terminals (ONTs) in a Gigabit Ethernet-based passive optical network ~~an E-PON structure~~, the encryption method comprising the steps of:

a) transmitting, when power is turned on and the OLT is driven, gate signals to the ONTs in order to detect ONTs connected through a transmission medium;

b) transmitting, by the ONTs, registration requirement signals and RSA public keys corresponding to the gate signal;

c) ~~registering~~ ~~registering~~, by the OLT, the ONTs in accordance with the registration requirement signals transmitted from the ONTs, assigning Logical Link IDs (LLIDs) with respect to the ONTs, and transmitting information for the assignment to the ONTs;

d) encrypting, by the OLT, secret keys by means of the public keys and transmitting the encrypted secret keys to the ONTs;

e) decrypting, by the ONTs, the encrypted secret keys transmitted from the OLT by means of private keys residing in an ONT key management unit ONT for managing a public key and a private key;

f) confirming, by the OLT and the ONTs, mutual sharing of the public keys and the secret keys, the OLT assigning bandwidth necessary for data transmission to the ONTs;

g) encrypting, by the OLT, data by means of the secret keys and transmitting the encrypted data to the ONTs; and

h) decrypting, by the ONTs, the encrypted data transmitted from the OLT by means of the decrypted secret keys.

15. (Currently Amended) An encryption method for transferring data by an Optical Line Terminal (OLT) in a Gigabit Ethernet-based passive optical network ~~an E-PON structure~~, the encryption method comprising the steps of:

transmitting, when power is turned on and the OLT is driven, gate signals through a transmission medium;

receiving registration requirement signals and RSA public keys corresponding to the gate signals;

~~registering~~ ~~registrating~~ the received registration requirement signals,

assigning respective Logical Link IDs (LLIDs) with respect to the registration requirement signals;

transmitting information for the assignment;

encrypting secret keys by means of the public keys and transmitting the encrypted secret keys;

confirming mutual sharing of the public keys and the secret keys;

assigning bandwidths necessary for data transmission;

encrypting data using the secret keys; and

transmitting the encrypted data.

3. The following is an examiner's statement of reasons for allowance: The prior art of record discloses a digital content protection method comprising encrypting private content key by content provider with public key of content receiver; transmitting the encrypted private content key to the content receivers; decrypting the encrypted private content key by the content receiver using a private key associated with the public key; and decrypting the encrypted content using the decrypted private content key. However, the prior art of record does not explicitly

disclose utilizing the conventional content protection method in a Gigabit Ethernet-based Passive Optical Network (GE-PON) utilizing Optical Line Terminal in light of features disclosed in independent claims 1, 10, 12 and 15.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/759,719

Page 7

Art Unit: 2131

Supervisory Patent Examiner, Art Unit 2131

Primary Examiner
Art Unit 2131

/S. C./